

## APPLICATION UNDER UNITED STATES PATENT LAWS

Atty. Dkt. No. PM 276662/2980355US/VK  
(M#)

Invention: INTERNET/INTRANET ACCESS MECHANISM

Inventor (s): AALTO, Mika  
LAKSO, Marja  
NYMAN, Kai

Pillsbury Winthrop LLP  
Intellectual Property Group  
1100 New York Avenue, NW  
Ninth Floor  
Washington, DC 20005-3918  
Attorneys  
Telephone: (202) 861-3000

This is a:

- ☐ Provisional Application
- ☐ Regular Utility Application
- ☐ Continuing Application  
☒ The contents of the parent are incorporated  
by reference
- ☒ PCT National Phase Application
- ☐ Design Application
- ☐ Reissue Application
- ☐ Plant Application
- ☐ Substitute Specification  
Sub. Spec Filed \_\_\_\_\_  
in App. No. \_\_\_\_\_ / \_\_\_\_\_
- ☐ Marked up Specification re  
Sub. Spec. filed \_\_\_\_\_  
In App. No. \_\_\_\_\_ / \_\_\_\_\_

## SPECIFICATION

1/PAT.

## Internet/intranet access mechanism

INSAI

### Background of the invention

The invention relates to a mechanism for accessing the Internet via an ATM (Asynchronous Transfer Mode) network. Within the context of this application, 'Internet' should be interpreted broadly to cover any large-area networks using Internet Protocols (IP). Especially it is the applicant's intention to include future developments, such as Internet 2 or NGI ('Next generation Internet'), and corporate networks, commonly referred to as intranets or ex-

tranets.

10 A person designing an Internet access mechanism faces several issues, such as interoperability, security, billing, economic use of IP addresses, and how to make the best use of installed equipment, etc.

From references [1, Kwok et al.] and [2, Nilsson et al.] are known Internet access mechanisms for connecting each of several customer premises equipment (abbreviated "CPE") via an ATM network to one of several service providers (SP). The concept of service provider comprises Internet service providers (ISP), content providers (CP, for video-on-demand, etc.), and corporate network servers (CNS, for telecommuting, etc.)

Referring to Fig. 1, CPEs are connected to the ATM network at network termination points (NT). A typical NT, such as NT1 in Fig. 1, is a network gateway having a network interface for the customer's local area network, LAN, and another interface towards the ATM network. Alternatively, a personal computer PC or a workstation WS can be connected directly (without a LAN) to the ATM network by means of an ATM/ADSL adapter card (shown as NT2), which in this case is the NT. In both cases, there is a well-defined NT for each CPE (although one NT may serve several CPEs). According to both cited references, the network comprises an access server function, or ASF, having a connection to each NT and each SP such that each NT has a permanent connection or a permanent virtual connection to the ASF. The wording 'access server function' implies that the ASF can be a dedicated network element or it can be integrated into or co-located with another network element, such as an ATM switch. In the cited references, the ASF has been referred to as an 'access node'/'DSLAM' (digital subscriber line access multiplexer) or an 'edge router'. It should be noted that the difference between 'permanent connection' and 'permanent virtual connection' has become rather blurred and later in this application, only 'permanent virtual connection' (PVC) will be used.

A problem of the known Internet access mechanisms is that they do not give a satisfactory answer to following problem: How can a specific end-user be connected to the desired service provider with a minimal number of permanent virtual circuits (PVCs) with a possibility of end-user authentication taking place only at the ends of the PVCs (not necessarily at the ASF)?

### Disclosure of the invention

An object of the invention is to solve or at least minimise the problem associated with the prior art access mechanisms. The object is achieved with a method and equipment which are characterized by what is disclosed in the attached independent claims. Preferred embodiments of the invention are disclosed in the attached dependent claims.

The invention is based on establishing a tunnelling protocol on the permanent virtual connection between each CPE or NT and the ASF, wherein the tunnelling protocol is able to support an integrated signalling protocol. Selecting an appropriate SP is based on the integrated signalling protocol. Routing to the selected SP is performed by the ASF. Finally, the ASF connects the CPE or NT to the selected SP using the integrated signalling protocol.

Within the context of this application, 'tunnelling protocol' refers to a protocol which allows creating and maintaining virtual private sessions via various network media such as IP, ATM, Frame Relay, etc. Correspondingly, 'integrated signalling protocol' (i.e. a signalling protocol integrated into the tunnelling protocol) refers to a control protocol which is used for creating, maintaining and releasing these sessions.

Implementation of the invention, however, raises two new issues: the ATM network must provide non-ATM functions in the ASF, and, unless properly dimensioned, the ASF can be a performance bottleneck. Such non-ATM functions performed by the ASF include functions above the ATM layer for the user connections, namely SAR/AAL5, the entire tunnelling protocol and selecting the SP by L2 signalling. These functions require appropriate administration. After a careful study of the pros and cons of the invention, it will be observed that there are situations where the advantages of the invention justify the added complexity of the ASF.

According to a preferred embodiment of the invention, one permanent virtual connection PVC is provided from the ASF to each SP. Alternatively, there is provided a pool of permanent virtual connections from the ASF to each SP. One PVC is allocated to each CPE from this pool. As a further op-

tion, it is possible to establish one switched virtual connection (SVC) from the ASF to each SP, on the basis of signalling which the ASF receives from the CPE via the tunnelling protocol.

- 5 The tunnelling protocol can be established only in response to detecting appropriate user activity in a CPE. Alternatively, the tunnelling protocol can be permanent and the integrated signalling is initiated and the user is authenticated only in response to detecting appropriate user activity in the CPE. According to a further preferred embodiment, the user is authenticated twice, first by the ASF using the tunnelling protocol, and then by the SP.

#### 10 **Brief description of the drawings**

The invention will be described in more detail by means of preferred embodiments with reference to the appended drawing in which:

Fig. 1 is a block diagram illustrating the Internet/intranet access mechanism according to the invention.

#### 15 **Detailed description of the invention**

- Fig. 1 a is block diagram comprising several customer premises equipment CPE, connected via network termination points NT to an access server function ASF according to the invention. The ASF can be a dedicated network element, or it can be integrated into or co-located with another network element, such as an ATM switch (which is known to a skilled person and not shown separately).

- 20 The ASF provides access from each CPE to several service providers SP, such as Internet service providers ISP, content providers CP and corporate networks CN. The invention requires no changes to the construction or operation of the SP equipment. Instead, the invention can be implemented in the ASF and the NT. There is preferably one permanent virtual connection (PVC) between each NT and the ASF.

- 30 In the embodiment shown in Fig. 1, there is one PVC from NT2 (in the workstation WS) to the ASF. Also, assuming that at least one of the personal computers PC is active, there is also a PVC from NT1 to the ASF. All the personal computers PC connected to the LAN share the PVC between NT1 and the ASF. According to a preferred embodiment of the invention, there is a tunnelling protocol, such as L2TP (Layer 2 Tunnelling Protocol), on the PVC from each active PC to the NT. The tunnelling protocol combines the sessions and signalling from all active PCs into a single tunnel from the NT to the ASF.
- 35

The tunnelling protocol must be able to support an integrated signalling protocol. The end user (i.e. the person using the CPE or a software agent being executed in the CPE) selects an appropriate SP by using the integrated signalling protocol. Routing to the selected SP is performed by the ASF. Finally, the ASF connects the CPE or NT to the selected SP using the integrated signalling protocol.

Reference 11 points to a preferred protocol stack at the NT and reference 12 points to a preferred protocol stack at the ASF. (The workstation WS connected to NT2 without a LAN needs a simpler protocol stack, consisting only of the right half of the protocol stack 11, i.e. PPP, L2TP, AAL5, ATM, and PHY.) Having point-to-point connectivity PPP over L2TP provides end-to-end security. In other words, it is not necessary for the ASF to authenticate the user, although the ATM operator may still choose to do so, in order to charge the subscriber for the duration of the session. However, even in this case, the end-user's choice of SP is not known to the ATM operator, which is a clear benefit to the owners of the SPs.

The preferred embodiment saves a considerable amount of PVCs over the prior art access mechanisms. Let us calculate an example case of 10 000 customers and 8 SPs and 20 ASFs (one ASF per 500 CPE). If all customers need access to all SPs, the prior art access mechanisms require a separate PVC for each customer/SP combination, i.e. in this example  $8 * 10\,000 = 80\,000$  PVCs. In comparison, the mechanism according to the invention requires a PVC only for each customer and each ASF/SP combination, i.e.  $10\,000 + 8 * 20 = 10\,160$  PVCs. (This number is not perfectly accurate since some ASF/SP connections can be switched virtual connections, SVC.)

According to an alternative embodiment of the invention, there is a separate PVC from each active PC between the NT and the ASF. In this case, implementation of the NT is easier because the tunnels from the PCs do not have to be combined (instead, all tunnels pass from the PCs, over the LAN, through the NT to the ASF).

The ATM operator's billing can be based on the time there is a PVC between the customer and the ASF. The invention simplifies this kind of billing because there is only one PVC from each customer. Also, when the customer changes the SP, a new PVC configuration is not needed.

Configuring and managing the NT device according to the invention, like the device itself, is rather simple. Only its LAN interface and its ATM

interface require configuration: an IP address, a subnet mask and an ATM PVC. The latter can be received automatically, using a technique known as ILMI (Interim Local Management Interface) as defined by ATM Forum UNI (User to Network Interface) 3.1. ILMI supports bidirectional exchange of management information between UNI management entities related to the ATM layer and physical layer parameters. Correspondingly, the LAN interface can be configured automatically by a process known as DHCP (Dynamic Host Configuration Protocol), as defined by the Internet Software Consortium.

The description only illustrates preferred embodiments of the invention. The invention is not, however, limited to these examples, but it may vary within the scope of the appended claims.

#### References:

1. Kwok, Timothy et al: *An Interoperable End-to-End Broadband Service Architecture over ASDL Systems*, version 1.0, 3 June, 1997, available at address <http://www.3com.com/xdsl/microwt.html> at the priority date of this application.
2. Nilsson, Patrik et al: *Anx -- High-speed Internet Access*, available at address [http://www.ericsson.com/Review/er1b\\_98/art4/art4.html](http://www.ericsson.com/Review/er1b_98/art4/art4.html) at the priority date of this application. The www address implies that reference 2 was printed in Ericsson Review magazine.

Both cited references are incorporated herein by reference.